The Evolution of Patch Management to Full Lifecycle Vulnerability Management
by Carl Banzhof, CTO, Citadel Security Software

One of the most compelling figures I've seen regarding the state of IT security comes from British computer security firm, Mi2G, which puts the economic impact of Internet-based intrusions for February 2004, just February, at an estimated $68 to $83 billion worldwide. With CERT®/CC reporting roughly 70 to 80 new IT system and network vulnerabilities per week and over 95% of the successful cyber attacks resulting from "known vulnerabilities or configuration errors where countermeasures were available" it is no wonder that most companies today are looking for ways to remove these flaws before they can be exploited and cause, at a minimum, disruption in service and in many cases, result in loss of sensitive data, economic damage, and tarnished reputation.

Today's enterprise is charged with the serious responsibility of weighing and managing security risk. It's the age-old formula that equates risk with *vulnerability x assets x occurrence rate*. Admittedly, most organizations do not have the luxury to change the IT assets they have, nor can they possibly control the occurrence rate of sabotage attempts. However, they *can* control vulnerabilities - what's going on inside their organization. With the plague of vulnerabilities that infest today's IT systems and networks – add to this the new job requirement placing senior level officers in charge of managing and mitigating risks to meet corporate governance standards, audits and regulatory mandates – it's no wonder that traditional patch management is no longer a viable option for comprehensive security practice.

Patch management is a reactive response to external risks and from a security perspective is inadequate because of the following key limitations:

Five Classes of Vulnerabilities

- Unsecured Accounts
  user account left dormant or possessing unnecessary privileges, i.e. Null Password, Admin no PW, no PW expiration…
- Unnecessary Services
  default applications or operating systems such as Telnet, Remote Access, Remote Exe…
- Backdoors
  programs that allow remote access and computer control such as NETBUS, BACKORIFICE, SUBSEVEN…
- Mis-configurations
  system and application vulnerabilities that are resolvable, i.e. NetBIOS null sessions...
- Software Defects
  the most discussed of vulnerabilities such as Hot-fixes, Patches…

1. The reactive "attack & patch" approach consumes unplanned and intensive levels of labor, requires long cycles, provides limited control at best, and actually increases the probability of undoing past securing efforts.
2. Patch management only addresses software defects which represent 20 to 30 percent of the critical system and network vulnerabilities found in most IT environments. Apart from exploitable software defects, there are four other classes of vulnerabilities that constitute the remaining 70 - 80 percent of critical vulnerabilities related to IT security. These include *unsecured accounts, backdoors, unnecessary services* and *mis-configurations*.
3. Patch management tools do not provide integration with commercially available vulnerability assessment tools – most patch management solutions have built-in

system scanners to identify needed software patches. Without this integration there is no systematic way to comprehensively identify and organize vulnerabilities into meaningful data that operational staff can act on.

From an operational standpoint patch management once seemed the best available option for addressing vulnerabilities. However, organizations today are realizing that patch management only addresses a very small piece of the vulnerability puzzle and is not enough to address their security concerns. The larger chunk of the equation involves a security process that in and of itself, spans multiple groups across an enterprise. I'm talking about your security team responsible for identifying and assessing vulnerabilities as well as your IT operations team, consisting of both network and systems administrators who are responsible for developing, testing, and deploying fixes for discovered vulnerabilities. For most companies this process is mostly manual resulting in a broken process that will not deliver the level of security, compliance, and confidence needed.

I believe the only way to improve a company's security posture and reduce risk is to automate as many processes as possible that are involved in identifying and resolving vulnerabilities. Enter *enterprise vulnerability management*, a full life cycle approach to take security efforts beyond patch management to a more proactive and holistic approach of asset classification, vulnerability identification and mitigation, and policy monitoring and enforcement.

Vulnerability management works on the basic premise that by removing the real problem – the vulnerability itself – you will minimize the number of threat occurrences to which your company is exposed, thus reducing overall risk. The following represents a best practices outline that eliminates system and network flaws through end-to-end vulnerability management across all 5 classes of vulnerabilities, ensuring the highest level of security with the least amount of interruption.

Best practices for closed loop vulnerability management

1. **Identify/Discover Systems & Devices** – inventory what aspects of your IT infrastructure – hardware, operating systems, applications and other technologies or services – are potentially the most vulnerable.
2. **Vulnerability Scanning** - proactively monitor and identify vulnerabilities specific to your environment. This step will allow for decisions regarding proactive and reactive steps necessary in order to remediate vulnerabilities.
3. **Vulnerability Review** - assess the exposure or liabilities caused by vulnerabilities for each of your assets – prioritize those that will cause the most risk to the business if exploited.
4. **Vulnerability Remediation** – counteract vulnerabilities by defining remediation actions and applying those actions through scheduled, automated end-to-end remediation.
5. **Ongoing Management** – close the loop on the vulnerabilities through policy definition and compliance checking.

The absence of an enterprise vulnerability management process creates a high-risk environment that is exposed to both internal and external security threats which can result in serious operational and financial consequences. Most security breaches could have been avoided if the proper vulnerability assessment and remediation actions had been enforced. Security attacks will only increase in frequency, degree and complexity, making vulnerability management a key IT priority.

The best advice I have for reducing today's security threats is to go beyond patch management by implementing a full lifecycle vulnerability management process and supporting software technologies to deliver an integrated approach across the different groups responsible for security processes – and automate as many steps as possible.

General Requirement for an Automated Vulnerability Remediation Solution

- Ease of use – product shall be easy to use and install.
- Interoperability with multiple security scanners – product shall integrate with multiple leading scanners on the market such as Harris STAT Scanner, ISS Internet Scanner, ISS System Scanner, Microsoft MBSA, Nessus, FoundStone, eEye Retina, and others. This will allow support of the AVR security lifecycle process of scanning, remediation and maintaining compliance with security policy.
- Vulnerability Aggregation – product shall aggregate data from multiple scanners to provide a true assessment of a security posture and expedite the vulnerability review process.
- Vulnerability analysis – product shall allow the user to review vulnerabilities and approve or disapprove for remediation
- Remediation Policy Enforcement – The product shall provide the capability to designate selected remediations at varying enforcement levels from Mandatory (required) to Forbidden (acceptable risk) which provides remediation enforcement from a centralized policy driven interface.
- Remediation – product shall remediate clients for all approved remediations for all five classes of vulnerabilities:
    - Accounts – Accounts with no PW, no PW expiration, known vendor supplied PW
    - Unnecessary Services – shutdown Telnet, KaZaa, other P2P, rsh, echo, etc.
    - Backdoors – remove backdoor programs such as MyDoom.A, W32.Beagle.I@mm, NETBUS, BACKORIFICE, SUBSEVEN, etc.
    - Mis-Configurations – correct configurations for NetBIOS shares, Anonymous FTP world read/write, hosts.equiv, etc.
    - Patches – patch buffer overruns, RPC-DCOM, SQL Injection, etc.
- Compliance Checking – product shall provide the capability to check compliancy against approved remediations.
- NIAP Common Criteria Certified to EAL3 - EAL3 provides a higher level of assurance that is required for IAVM tools. The IAVM product shall be developed to meet stringent security requirements. A vulnerability assessment of the product is also performed to meet EAL3.
- CVE Compliance – product shall be CVE compliant.
- Encrypted communications – product shall provide encrypted communications among distributed components.
- IAVM Support – product shall support any IAVA database source to respond and maintain compliance with IAVA bulletins.
- Device Support – product shall support multiple platforms including Windows, Linux and major Unix OS such as Solaris, AIX and HP-UX.
- Group Management – product shall allow grouping of devices to manage remediation and control access to devices.
- Roll-Based Access Control – product shall allow groups of devices to be managed based on roles to establish separation of roles different tasks such as vulnerability review and remediation of devices.
- Network Protection – product shall prevent disconnected / remote users from connecting to the internal protected network if they are not compliant with their required remediation. It shall also require the required remediation to be performed.
- Reporting – product shall provide multiple reports to determine remediation success and trending.
- Distributed Patch Repository - The product shall provide the capability to load balance and distribute the bandwidth associated for patch distribution to repositories installed in various strategic locations.
- Custom remedies - The product shall allow users the ability to customize any delivered remediation actions to fit a particular purpose as well as create new remediation actions from scratch.

- Microsoft Windows 2000 / 2003 Server Certified. The product shall be certified by Microsoft to run on Windows 2000 or 2003 Server editions.
- Multiple Sources of New Vulnerability Reporting – vendor shall monitor multiple sources of vulnerability reporting and quickly provide remediation to latest discovered vulnerabilities
- Security Team Monitoring Vulnerabilities and Exploits 24x7 – vendor shall have a dedicated team of security experts to monitor for new vulnerabilities and exploits 24x7
- Remedy library. - The product shall be delivered with tested and validated remediation actions for all platforms that the product supports. The library should be supported by a dedicated team of security professionals within the organization.
- Automatic Update Service – product shall securely provide up-to-date remedies for newly identified vulnerabilities on a regular basis.
- Embedded Security Center Portal – product shall have an embedded security portal that will provide quick access to security and product related information
- Remediate by Policy – product shall accurately deploy remediation based on security requirements without the need of a SCAN
- Application Remediation – product shall support remediation of applications like MS SQL, MS Exchange, IIS, MS Office, IE and others.
- Automated agent distribution – product shall support automated agent distribution to individual devices and groups of devices to facilitate ease of deployment.
- Remediation Templates – product shall support remediation groups to be used as templates to represent a specific security policy. Multiple templates may be applied to devices and templates should be exportable and sharable.
- Support Standard Hardening Policy – product shall deploy and maintain compliance for industry standard hardening policies, such as CIS Gold Standard, MS Hardening Guides, NSA Guides (STIG, etc.).
- Customization of Vulnerabilities and Remediations - Allows users to easily customize existing vulnerabilities and remediations.
- Patch Interdependency – the product shall calculate patch interdependencies and automatically deploy the patches needed based on the installed products and drivers.
- Patch Uninstall – product shall report if a patch was uninstalled or needs to be reapplied.
- Web-Based UI – product shall have a web-based user interface, the tool goes where the administrator goes